TOP SECRET "U"

TICOM/I 2

15(L)

INTERROGATION OF DR. HUETTENHAIN AND DR. FRICKE AT FLENSBURG 21 MAY 1945.

TICOM
loth June 1945

DISTRIBUTION.

British
Director
D.D.3.
D.D.4.
D.D.(N.S.)
D.D.(M.W.)
D.D.(A.S.)
A.D.(C.C.R.)(2)
Ccl. Leatham

Ticom
Chairman
S.A.C. (2) Copy sent DD(CSA) 14/6
Cdr. Bacon
Cdr. Mackenzie
Cdr. Tandy
W/Cdr. Oeser
Lt.Col. Johnson
Major Seaman
Lt. Eachus
Lt. Vance
Captain Cowan
Lt. Fehl
Ticom Files (2)

U.S.
OP-20-G (2) (via Lt. Pendergrass)
G-2 (via Lt. Col. Hilles)
S.S.A. (2)(via Major Seaman)
Director, S.I.D. ETOUSA (2)(via Lt.Col. Johnson)

NOTE: Regierungsrat Dr. Erich HUETTENHAIN was the best cryptographer at OKW/Chi. Dr. FRICKE was also at OKW/Chi. They were apprehended at Flensburg.

PRELIMINARY INVESTIGATION AND INTERROGATION AT O K W CONTROL COMMISSION FLENSBURG (21.5.45)

SUBJECT: REGIERUNGSRAT DR. ERICH HUETTENHAIN

Q. YOUR JOB AND INTERESTS?

A. STUDIED MATHS AND ASTRONOMY, WAS ASSISTANT AT A UNIVERSITY

Q. JOB AT CHI?

A. DIRECTOR OF CHI B IV THEORETICAL DECIPHERING DECIPHERING DEPARTMENTS DIVIDED INTO TWO PHASES, PRACTICAL DECYPHERING DONE BY A GROUP OF TECHNICIANS AND LINGUISTS ON CODES AND CIPHERS THAT HAD BEEN ALREADY BROKEN AND WAS BEING READ CURRENTLY WHILE THEORETICAL DECIPHERING WAS MORE OR LESS RESEARCH AND ATTEMPTS TO BREAK NEW CODES AND CIPHERS BY A GROUP OF MATHEMATICIANS.

Q. WHAT WORK WAS DONE ON SPECIFIC CODES AND CIPHERS?

A. FOUR BRANCHES OF MY DEPARTMENT WERE
1. MONITORING THE SECURITY OF OUR OWN CODES AND CIPHERS.
2. DESIGN AND CONSTRUCTION OF AUXILIARY EQUIPMENT FOR DECODING AND DECIPHERING FOREIGN CODES AND CIPHERS.
3. SOLUTION OF DIFFICULT CODES AND CIPHERS (CRYPTOGRAPHIC RESEARCH).
4. MAINTENANCE OF INSTRUCTIONAL AND TRAINING SCHOOLS FOR CRYPTOGRAPHY.

Q. DID YOU MAKE UP CODES AND CIPHERS?

A. IT WAS NOT MY JOB TO MAKE UP OUR OWN CODES. I MERELY TESTED THEIR SECURITY.

Q. WHAT TYPES OF ALLIED CODES AND CIPHERS WERE BROKEN?

A. MANY WERE WORKED ON AND SEVERAL WERE SOLVED.

Q. WHAT RUSSIAN TRAFFIC WAS WORKED ON?

A. 1. DIPLOMATIC - NONE IN THIS FIELD BECAUSE ONE TIME PADS WERE BEING USED. THIS TRAFFIC WAS ONLY OBSERVED AND SEARCHED FOR REPEATS TO GIVE POSSIBLE BREAKS. I DIDN'T WORK ON THIS BECAUSE IT WAS REALISED THAT IT COULD NOT BE BROKEN.

2. MILITARY - WE SOLVED A NUMBER OF THESE.
TYPES - 1. ZZ LETTER FOR LETTER SUBSTITUTION
2. ZZZ SMALL CODE BOOK, THREE FIGURE, ENCODED BY MEANS OF A TAUSCHTAFEL.
3. ZZZZ CODE SENTENCE BOOK, ENCODED EACH DAY WITH PAGE AND LINE CHANGED.
4. ZZZZZ FIVE LETTER CODE, ENCODED BY ZAHLENWURM (ADDITION OR SUBTRACTION OF FIVE FIGURES).

RUSSIAN ADDER SYSTEM SECURITY WAS VERY BAD AT FIRST AND ALLOWED FOR BREAKING. DURING THE LAST SIX MONTHS THIS CODE COULD NOT BE BROKEN. I WAS FORMERLY THE DIPLOMATIC EXPERT; OBLT. SCHUBERT IS THE EXPERT ON RUSSIAN ARMY CODES. HE IS AT PRESENT IN FLENSBURG.

Q. DID THE RUSSIANS USE MACHINES?

A. THEY HAVE A MACHINE MODELLED AFTER THE FRENCH PATTERN 211, HAGELIN TYPE.

Q. DID YOU HAVE ANY SUCCESS WITH THIS MACHINE?

A. WE CAPTURED A MACHINE BUT DID NOT INTERCEPT ANY TRAFFIC. THEY ALSO HAVE ANOTHER MACHINE, FUNKFERNSCHREIBER, WHICH ENCODES DURING TRANSMISSION. IT USES THE INTERNATIONAL FIVE IMPULSE TELEPRINTERCODE.

Q. DID THE RUSSIANS USE THIS MACHINE MUCH?

A. IT BECAME INCREASINGLY IMPORTANT DURING THE LAST $1\frac{1}{2}$ YEARS.

Q. WHAT UNITS USED IT?

A. ONLY THE HIGHEST STAFFS, PRESS, AND DIPLOMATIC SERVICES.

Q. ANYTHING ELSE?

A. THEY HAD FINALLY A SECRET R/T OF WHICH ONLY A SMALL PART OF A FEW MESSAGES WERE READ. THIS WAS PROBABLY USED IN DIPLOMATIC AND ECONOMIC CIRCLES. WE WERE NOT SURE BECAUSE ONLY BITS WERE READ. WE KNOW HOWEVER THAT THE RUSSIANS WERE EXPERIMENTING WITH IT.

Q. WHAT ARE THE PRINCIPLES OF THIS MACHINE?

A. SYSTEM IS KNOWN AS TIGER-STEDT AND IS THE SAME AS THAT USED BY AMERICAN MUSTANG GROUPS. SPOKEN PLAIN TEXT IS OSCILLOGRAPHED ON STEEL TAPE AND LENGTHS OF TAPE ARE CUT AND THEN REASSEMBLED.

Q. WHAT WORK WAS DONE ON BRITISH AND AMERICAN CODES AND CIPHERS?

A. DIPLOMATIC - MOST OF THE AMERICAN STRIP CIPHER WAS READ. STRIP CIPHER WAS USED BY THE MILITARY AS WELL AS BY THE DIPLOMATIC.

Q. WAS THIS DIPLOMATIC USED MUCH?

A. USED A GREAT DEAL IN LINIE AND KREIS (STERN) SYSTEMS OF RADIO. 80% OF THE BREAKS CAME ABOUT AS A RESULT OF MISTAKES BY THE USERS. THE SYSTEMS ARE EXCELLENT BUT ARE GIVEN AWAY BY THE USERS.

Q. ARE OTHER SYSTEMS USED ON THE SAME LINKS?

A. YES.

Q. WHAT ARE THE PERCENTAGES OF STRIP AND OTHER TRAFFIC?

A. I AM NOT CERTAIN OF THE EXACT PERCENTAGES, BUT AT FIRST THERE WAS NOT MUCH STRIP. ABOUT $1\frac{1}{2}$ YEARS AGO (JAN 1944) THE STRIP SYSTEM WAS MADE MORE DIFFICULT SO THAT ONLY CERTAIN LINES COULD BE READ, FOR INSTANCE BERNE TO LONDON. NEAR THE END NOTHING COULD BE READ. ORIGINALLY THIRTY STRIPS WERE USED, THEN THE SYSTEM WAS MODIFIED BY REMOVING VARYING NUMBERS OF STRIPS FOR EACH MESSAGE.

Q. WHAT TYPES OF MISTAKES LED TO BREAKING?

A. THE ENCODING OF THE SAME MESSAGE IN TWO DIFFERENT CIPHERS, ONE OF WHICH WAS STRIP AND THE OTHER ONE WHICH WAS BEING READ. STEREOTYPED BEGINNINGS, IDIOMATIC PHRASES, AND ROUTINE MESSAGES. THE SAME MESSAGE TO VARIOUS ADDRESSES IN DIFFERENT STRIP SYSTEMS.

Q. WERE OTHER TYPES OF DIPLOMATIC TRAFFIC BROKEN?

A. ENCIPHERED CODE, USING CONVERSION TABLES. BETWEEN TWENTY AND THIRTY TABLES WERE AVAILABLE FOR EACH MESSAGE, AND THERE WERE TEN DIFFERENT CONVERSION SYSTEMS, WHICH WERE CHANGED QUARTERLY. IT TOOK ABOUT TWO MONTHS TO BUILD UP TABLES, SO THAT WE COULD ONLY READ THE TRAFFIC CURRENTLY DURING THE LAST MONTH OF THE PERIOD.

Q. WHAT TYPE OF CONVERSION TABLE WAS USED?

A. THERE WERE RECTANGLES OF APPROXIMATELY TWENTY COLUMNS OF RANDOM MIXED ALPHABETS WITH THE PLAIN TEXT ALPHABET RUNNING VERTICALLY ALONG THE SIDE. AT FIRST THE CODE GROUPS WERE MADE UP OF FIVE LETTERS IN THE SEQUENCE - CONS. VOWEL CONS. AT FIRST VOWELS COULD BE CONVERTED ONLY TO VOWELS, BUT LATER THEY COULD ALSO BE CONVERTED TO CONSONANTS. THE ORIGINAL VOWEL TO VOWEL CONVERSION WAS A WEAK POINT IN THAT IT REDUCED THE POSSIBILITIES. ABOUT THERTY GROUPS WERE ENCIPHERED PER TABLE, THEN AN ENCIPHERED INDICATOR (USING OLD TABLE) REFERRED TO THE NEXT TABLE. THIS INDICATOR WAS ALSO USED IN BREAKING AS IT USUALLY OCCURRED WITH THE SAME INTERVAL.

Q. WHAT OTHER DIPLOMATIC TYPES WERE BROKEN?

A. UNENCIPHERED FIVE LETTER CODE, WHICH HAS BEEN IN USE SINCE 1920. THIS WAS NOT IMPORTANT TRAFFIC. WE ALSO BROKE A DOUBLE TRANSPOSITION SYSTEM BY MEANS OF DEPTH.

Q. WHAT TYPE OF MILITARY CODES, CIPHERS, OR MACHINE CIPHERS WERE BROKEN?

A. THE MAIN MACHINE USED, AND BROKEN WAS THE AMERICAN HAGELIN WHICH WAS BROKEN ONLY WHEN ERRORS OCCURRED, FOR INSTANCE - THE SAME INDICATORS USED TWICE, OR REPEAT OF MESSAGE AS RESULT OF WRONG WHEEL SETTING (OBLT. SCHUBERT IS THE EXPERT ON THIS). COMMON AND REGULAR SOLUTION IMPOSSIBLE. HAGELIN OFFERED US HIS MACHINE FIRST IN 1934 BUT WE REFUSED IT BECAUSE MISTAKES COULD BE MADE AS THE RESULT OF WHICH THE MACHINE COULD BE BROKEN. THE MACHINE WAS MUCH SIMPLER THEN.

Q. WHAT OTHER TYPES OF MACHINES WERE WORKED ON?

A. I KNOW OF NO OTHER TYPE OF AMERICAN MACHINE, BUT THE BRITISH TYPEX IS KNOWN. IT WAS NOT BROKEN, AND SO FAR AS WE KNOW CANNOT BE SOLVED UNLESS THE WHEEL POSITIONS ARE KNOWN.

Q. WAS ANY CONCERTED ATTEMPT MADE TO BREAK TYPEX?

A. WE HAVE THE ENIGMA WHICH IS SIMILAR TO THE TYPEX, AND AS WE BELIEVE THAT THE ENIGMA CANNOT BE SOLVED NO GREAT EFFORT WAS MADE TO SOLVE TYPEX. TYPEX HAS SEVEN WHEELS AND WE THEREFORE BELIEVE IT TO BE MORE SECURE THAN OUR ENIGMA. ENIGMA WHEN USED ACCORDING TO INSTRUCTIONS IS UNBREAKABLE. IT MIGHT BE BROKEN IF A VAST HOLLERITH COMPLEX IS USED BUT THIS IS ONLY SLIGHTLY POSSIBLE!

Q. BY WHAT METHOD COULD ENIGMA BE BROKEN?

A. THE WIRING OF THE WHEELS MUST BE KNOWN

Q. IS THE WIRING FIXED?

A. IT IS GENERALLY FIXED BUT DURING THE YEARS IT HAS CHANGED.

Q. IF THE WIRING WERE KNOWN WHAT METHOD WOULD YOU USE?

A. LARGE CATALOGUES MUST BE BUILT UP BY ENCODING THE LETTER E IN ALL POSITIONS OF THE MACHINE (UNSTECKERED). THE LETTER E HAS A FREQUENCY OF 18% IN GERMAN PLAIN TEXT, AND THIS IS THE BASIS FOR SOLUTION.

(AT THIS POINT THE INTERROGATION WAS DISCONTINUED ALONG THESE LINES BECAUSE IT WAS FELT THAT A MORE DETAILED INTERROGATION WOULD BE NECESSARY LATER)

Q. WHAT IS YOUR PRESENT JOB?

A. I HAVE NONE.

Q. DO YOU HAVE ANY RELATION TO THE GROUP AT HUSUM?

A. NO.

THE REGIERUNGSRAT MADE THIS CLOSING REMARK:

THE SECURITY OF THE ENIGMA WAS NEVER COMPLETELY TESTED BECAUSE THE MACHINE WAS THOUGHT TO BE SECURE. WE CONCLUDED THAT FURTHER WORK ON THE MACHINE WAS NOT NECESSARY, BECAUSE IT IS SECURE AS IT IS.

SUBJECT: SONDERFUEHRER DR. WALTER FRICKE

Q. WHAT IS YOUR DEPARTMENT OF CHI?

A. CHI. A II THE PRODUCTION OF CODES AND CIPHERS.

Q. WHAT CODES AND CIPHERS?

A. ALMOST ENTIRELY ARMY.

Q. WHAT TYPES OF CODES AND CIPHERS?

A. FUNKTAFELN AND SCHLUESSELTAFELN (THREE LETTER).

Q. WERE MACHINES USED IN THE PRODUCTION OF THESE?

A. SCHLUESSELTAFELN WERE MADE WITH HOLLERITH MACHINES.

Q. HOW MANY TAFELN WERE MADE?

A. ORIGINALLY EACH DIVISION HAD THREE OR FOUR, AND THE SAME ONE MIGHT BE USED BY SEVERAL DIVISIONS. LATELY, THOUGH, DIFFICULTIES OF DISTRIBUTION AND SHORTAGES ALLOWED FOR ONLY ONE PER DIVISION.

Q. DID YOU MAKE UP ENIGMA KEYS?

A. YES WE DID; BUT ONLY FOR THE ARMY THREE WHEEL MACHINES. THE NAVY AND AIR FORCE MADE THEIR OWN KEYS.

Q. WHAT WAS THE DIFFERENCE IN THE KEYS?

A. THERE WAS NO DIFFERENCE BETWEEN ARMY AND AIR FORCE ENIGMA KEYS. THE AIR FORCE USED A PLUGABLE UMKEHRWALZE. FORMERLY THE ARMY USED SOME OF THESE, FOR FIXED STATIONS.

Q. HOW WERE THE KEYS MADE UP?

A. ALL SIXTY WHEEL ORDERS WERE WRITTEN DOWN ON SLIPS OF PAPER AND DRAWN AT RANDOM. RANDOM THREE LETTER GROUPS FOR RING-STELLUNG WERE DRAWN IN THE SAME MANNER. TEN STECKER PAIRS WERE SELECTED BY SEVERAL PEOPLE. ALL THIS DONE BY HAND, NO MACHINES EMPLOYED.

Q. HOW DID THE AIR FORCE AND THE NAVY MAKE UP THEIR KEYS?

A. THE AIR FORCE GOT THEIR INSTRUCTIONS FROM US. THEY SHOULD HAVE USED THE SAME PROCEDURE, AT ANY RATE THEY HAD NO BETTER METHOD.

((INTERROGATION TERMINATED AT THIS JUNCTURE AS ARRANGEMENTS HAD BEEN MADE FOR THIS SUBJECT TO BE SENT TO THE U.K. ALONG WITH DR. HUETTENHAIN))

(Signed) E.K. MORRISON, Major, I.C.
LOUIS LAPTOOK, 1st Lt., Sig.C., U.S. Army